OPERATIONS SECURITY

OPSEC

OVERVIEW

- OPSEC History
  - OPERATION PURPLE DRAGON
- Why OPSEC?
- What is OPSEC?
  - Definition
  - 5-Step Process
    - Critical Information
    - Indicators
    - Threats
    - Countermeasures
- OPSEC POC's

OPERATION PURPLE DRAGON

- Small team established during the Vietnam War, code named: “PURPLE DRAGON”
- Team’s mission: determine how enemy was obtaining advance information on B-52 bombing missions
- Traditional security and intelligence countermeasures programs were already in existence
  - Problem: these programs didn’t protect mission critical information or deny operational indicators relating to intentions and capabilities to the enemy

OPERATION PURPLE DRAGON

- Team developed methodology of analyzing U.S. operations from adversaries viewpoint
  - They discovered that Viet Cong had been receiving mission times and locations on a regular basis
    - U.S. pilots were required to file flight plans with Manila civilian Air Controllers
    - Information subsequently passed to Hanoi via International Air Traffic Controlled Channels
- Team recommended corrective actions to local commanders. Operation was successful.
- Process became known as: “Operations Security”

WHY OPSEC ?

To DENY adversaries information

- **Publications governing Air Force OPSEC Program:**
  - **Chairman Joint Chiefs Special Instruction 3213.01A**
  - **Joint Pub 3-54**
  - **Air Force Policy Directive 10-11**
  - **Air Force Instruction 10-1101**
  - **Army Regulation 530-1**
  - **Supplements to OPLANS**

OPSEC DEFINITION

OPSEC is a process of identifying critical information and analyzing friendly actions attendant to military operations and other activities to:

- **Identify those actions that can be observed by potential adversaries.**
- **Determine indicators that could be interpreted or pieced together to derive critical information in time to be useful to an adversary.**

- **Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.**

AFI 10-1101

OPSEC DEFINITION

In other words..

A process to *deny an adversary Critical Information* deduced from Indicators associated with planning and conduct of military operations.

OPSEC PROCESS

ID CRITICAL INFORMATION

ANALYZE THREATS

ANALYZE VULNERABILITIES

ASSESS RISK

APPLY COUNTER-MEASURES

CRITICAL INFORMATION

CRITICAL INFORMATION

Specific *facts* about friendly intentions or operations vitally needed by adversaries to act

Indicators are *observable activities* or information derived from *open sources* that when pieced together can possibly reveal critical information

8th AF CRITICAL INFORMATION

Critical Information (CI) Categories:

1. GENERAL
2. OPERATIONS
3. INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (ISR)
4. COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS (C4)
5. MOBILITY
6. LOGISTICS
7. RESOURCE PROTECTION

8th AF
OPSEC INDICATORS

Examples:

- Extended Working Hours
- Increased Secure Communications
- Move to the RTOC
- Issue of Special Uniforms and Equipment
- Telephone Recalls

8th AF
OPSEC THREATS

The Threat to Barksdale AFB is considered: LOW

Examples:

- **Foreign College Students**
- **Foreign Military Visitors**
- **Tail Watchers**
- **Internet (NIPRNET, E-MAIL, CHAT, etc.)**
- **Telephone/Radio/Pager Monitoring**

OPSEC COUNTERMEASURES

What can you do to protect Critical Information?

Examples:

- **Be aware of what's on the CI list**
- **Use STU-IIIs to discuss CI related items**
  - **Better yet, talk in person if nearby**
- **Use secure fax/e-mail if possible**
- **Shred all work related paper waste**
- **Don't talk shop off duty--You never know who is listening in**